Winter 2026

Liminal

Account Takeover Prevention in Banking

Third-Party Fraud



link Index™ Report

This report is licensed for reprint distribution by entersekt

Copyright © 2026 Liminal Strategy, Inc. | Liminal.co This report may not be reproduced without permission from Liminal. Citation policy

Contents

Navigation – click the Liminal logo to return to this page.

Introduction

Market Overview 3

Vendor Landscape 5

Use Case Overview 7

Market Overview: Account Takeover Prevention 8

Liminal's Use Case Methodology: Key Product Requirements 9

ATO Buyer Personas 10

Chief Risk Officer 11

Chief Financial Officer 12

Head of Fraud Prevention 13

End-to-End Solutions Prevent ATO, Detect Fraud, and Protect Banks From ATO Exploitation 14

Market Overview 16

ATO Key Insights 17

ATO Operational Barriers 18

Key Purchasing Criteria for ATO Solutions 19

ATO Future Outlook 20

Link Index 21

ATO Vendor Product Evaluation 22

ATO Vendor Strategy Evaluation 23

ATO Vendor Market Presence Evaluation 24

ATO Vendor Evaluation 25

Leadership Thresholds for ATO: Minimum product execution threshold 26

Leadership Thresholds for ATO: Minimum strategy threshold 27

ATO Leading Vendors 28

15 Leaders, 258 Evaluated Vendors 29

Link Index Leading Vendors for Account Takeover Prevention in Banking in 2025 30

ATO Leading Vendor Characteristics 31

ATO Leading Vendor Future Outlook 32

Vendor Overview 33

Entersekt 34

Appendix 36

Market Presence Survey Demographics 37

Link Index Methodology Exceptional, Excellent, Strong Scoring Buckets Definitions 38

Product Capability Definitions 39

Link Index Methodology: Product 42

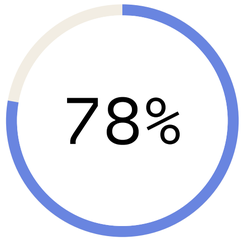
Link Index Methodology: Strategy 43

Link Index Methodology: Market Presence 44

About Liminal 45

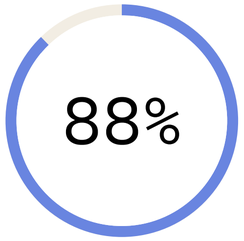
Market Overview

Key Takeaways



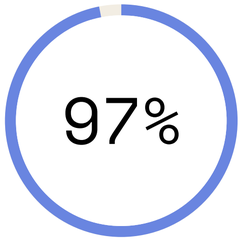
Mobile Fraud Prevention

78% of practitioners expect to increase mobile fraud prevention budgets within two years



Security Tradeoffs

88% of practitioners deprioritize stronger safeguards to avoid user friction



Authentication Effectiveness

97% of practitioners confirm authentication's effectiveness in reducing risk, making it central to ATO defense

01

Fragmented Threat Landscape Forces Organizations to Defend Against Multiple Attack Vectors[1]

Organizations face a broad range of ATO threats without a single dominant vector. Credential stuffing (27%), social engineering (26%), and man-in-the-middle attacks (26%) account for most incidents, followed by SIM swap (21%) and phishing (19%). This distribution complicates resource allocation and leaves security teams overextended across multiple fronts.

02

Mobile Vulnerabilities Drive Increased Investment in Fraud Protection[1]

Mobile environments remain the most targeted channel, with attacks occurring 2.5× more often than on desktop. As a result, 78% of practitioners expect to increase mobile fraud prevention budgets within two years. Rising threats across third-party partners (76.7%), APIs (74%), and call centers (65.8%) highlight the need for cross-channel defense strategies.

03

Automation and Authentication Strengthen Recovery Capabilities[1]

Authentication has become central to ATO defense, with 97% of practitioners confirming its effectiveness in reducing risk. Automated identity re-verification is now used by 81% of practitioners, compared to only 21% relying on manual review, demonstrating the shift toward scalable, low-touch recovery.

04

Balancing Security With Customer Experience Remains a Persistent Tradeoff[1]

While 42% of practitioners rate their current recovery processes as ineffective, 88% deprioritize stronger safeguards to avoid user friction. Nevertheless, 61% report that improving ATO response boosted customer trust, underscoring the importance of recovery approaches that maintain both protection and usability.

1 Third Party Fraud Buyer Demand Survey, August 2025 (N=73)

Market Overview



Current Challenges[1]

Fragmented Threat Landscape and Resource Constraints Limit Effective Defense

Organizations face multiple concurrent ATO attack types, with credential-based, social engineering, and man-in-the-middle attacks each accounting for roughly one-quarter of incidents. The absence of a single dominant threat vector makes it difficult to prioritize defenses and allocate resources effectively, leaving security teams strained.

Rising Mobile and Third-Party Vulnerabilities Expand the Attack Surface

Mobile channels are 2.5× more susceptible to attack than desktop environments, while 77% of practitioners anticipate increasing risk from third-party partners and API integrations. The expansion of attack entry points across devices and ecosystems complicates prevention strategies and increases the likelihood of undetected compromise.

Repeat Targeting of Compromised Accounts Prolongs Exposure

Ninety-five percent of practitioners report persistent attacks on previously compromised accounts, indicating that breached credentials often remain in circulation and continue to be exploited. This repeated targeting highlights the limitations of single-instance remediation and the need for continuous monitoring and adaptive controls.

Coordination Gaps and Ownership Ambiguity Hinder Incident Response

Ambiguous team ownership undermines response efficiency. Although IT security teams manage most prevention efforts (78%), 69% of practitioners cite unclear accountability as a leading cause of delayed decision-making and resolution. This lack of coordination creates operational inefficiencies that heighten the overall impact of ATO incidents.

Future Demands[1]

Escalating Multi-Vector Risks Drive Demand for Layered Defenses and AI-Adapted Detection

Organizations continue to face exposure from multiple attack vectors, creating the need for layered defenses. Ninety-six percent of practitioners identify generative AI as an escalating risk, prompting proactive investment in adaptive detection. Sixty-six percent plan to increase model tuning and signal diversity, while 34% intend to develop new detection techniques—indicating that all practitioners are preparing to counter AI-driven ATO threats.

Preference for Unified Platforms and Orchestration to Simplify Threat Mitigation Efforts

Buyers are increasingly prioritizing integrated solutions, with 88% of practitioners favoring consolidated platforms or orchestration layers. This reflects a growing demand for unified ecosystems that improve coordination and operational efficiency across fraud prevention functions. However, the number of ATO vendors used by organizations is still expected to increase slightly (6%) over the next year, suggesting that despite the preference for consolidation, technology stacks will remain diversified.

Focus on Third-Party Channels Signals Anticipated Investment in Partner Risk Controls

Although only 7% of practitioners viewed third-party partners as the leading source of ATO risk in the past year, investment priorities are shifting. Eighty percent of organizations plan to increase spending on fraud prevention targeting partner and affiliate ecosystems within two years. This change signals heightened recognition that indirect exposure through third parties represents an emerging vulnerability that requires preemptive protection.

Leading Key Purchasing Criteria (KPC) for ATO Solutions[1]

Data Quality

98.63% of ATO Practitioners consider data quality important when selecting a solution.

End-Customer Experience

7.26% of ATO Practitioners consider accuracy important when selecting a solution.

1 Third Party Fraud Buyer Demand Survey, August 2025 (N=73)

Vendor Landscape

Liminal's Account Takeover Prevention in Banking vendor landscape analysis identifies the top 15 vendors addressing the complexity of verifying real-world identities in digital environments

Organizations face an increasingly complex threat environment marked by diverse attack vectors, expanding mobile and third-party vulnerabilities, and repeated exploitation of compromised accounts—all exacerbated by unclear ownership and limited resources that undermine coordinated, timely defense. Vendors within this landscape offer specialized approaches, categorized into three primary groups: End-to-End Fraud and Risk Platforms, Authentication and Access Management Platforms, and Behavioral and Device Intelligence Specialists.

Landscape Analysis

End-to-End Fraud and Risk Platforms

These vendors offer comprehensive fraud prevention, identity verification, and transaction risk management. Their platforms use integrated behavioral analytics, authentication orchestration, and AI-driven anomaly detection to guard against ATO and related fraud. They are typically adopted by large financial institutions for unified, scalable fraud management frameworks that meet enterprise compliance needs.

Authentication and Access Management Platforms

These platforms enhance user security and session integrity via adaptive authentication, continuous risk assessment, and MFA. They reduce credential fraud by dynamically adjusting authentication based on user behavior, device health, and contextual risk, ideal for institutions seeking secure, low-friction user experiences.

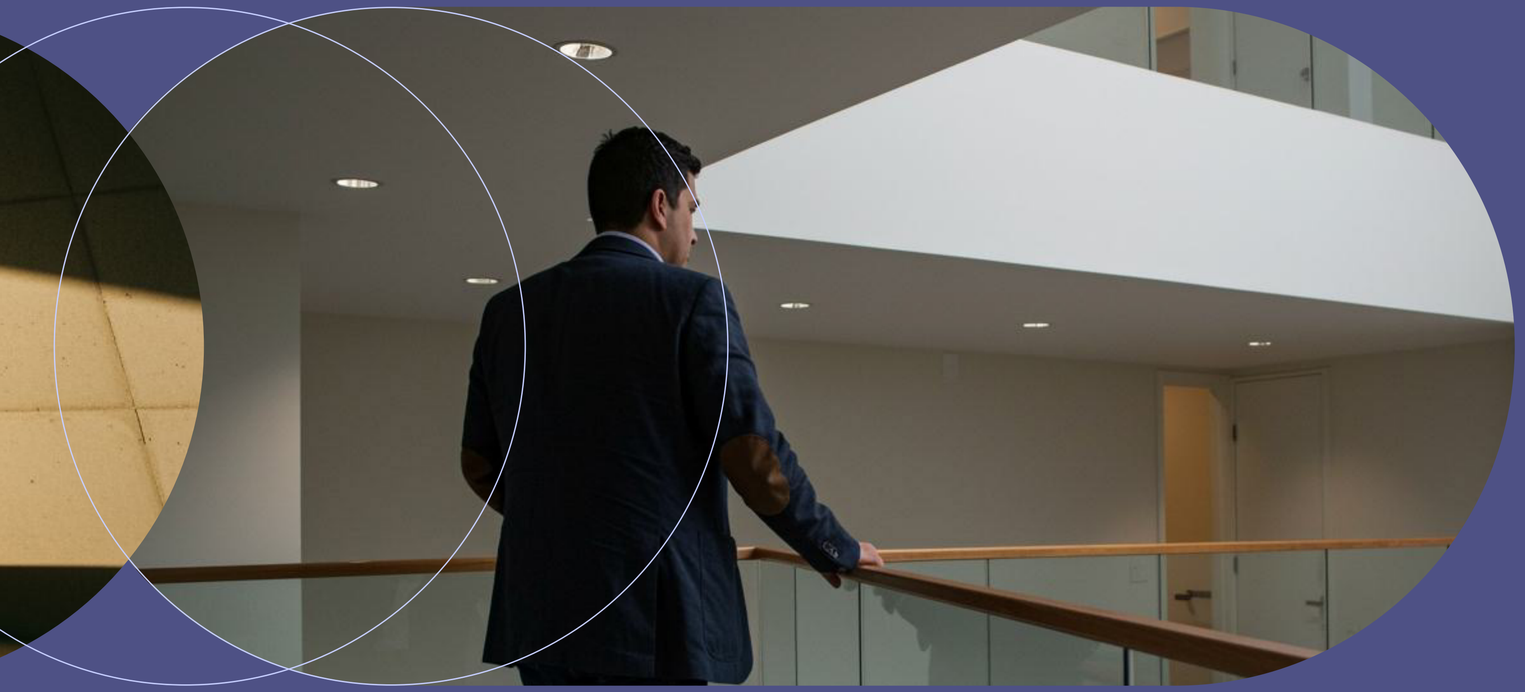
Behavioral and Device Intelligence Specialists

These vendors use behavioral biometrics, device fingerprinting, and network analytics to detect anomalous activity signaling account compromise. They analyze interaction patterns, geolocation, and device consistency to identify potential takeovers in real time. Their main strength is precision threat detection and flexible integration for digital banking, payments, and eCommerce.

Vendor Landscape

15 Leading Vendors for ATO

AppGate
BioCatch
callsign
DATAVISOR
descope
entersekt
EQUIFAX
experian
incode
LexisNexis RISK SOLUTIONS
PingIdentity
Prove
sumsub
transmit security
TransUnion



01

Use Case Overview

Market Overview: Account Takeover Prevention

Account Takeover Prevention Strengthens Security Measures and Protects Customer Trust in Banking

Account takeover is a form of fraud in which cybercriminals gain unauthorized access to an online account and assume control over it. Once access is secured, the attacker can perform unauthorized transactions, steal personal or financial information, and use the compromised account to commit further fraudulent activities. This type of fraud often begins through methods such as phishing, credential stuffing, or the exploitation of weak or reused passwords. The primary goal of account takeover prevention is to detect and block unauthorized access before any damage occurs, preserving customer assets and the institution's reputation.

In banking, effective account takeover prevention is critical to maintaining trust and regulatory compliance. By proactively detecting and mitigating threats, institutions can reduce financial losses, avoid legal repercussions, and ensure continuous service availability. The market for fraud prevention in banking has evolved into an ongoing contest between increasingly sophisticated cyber threats and advanced defensive strategies. Financial institutions are turning to solutions that combine artificial intelligence, predictive analytics, and behavioral biometrics to combat complex attack techniques.

Growing complexity in cybercriminal tactics has driven the adoption of more advanced security approaches. Regulations that limit data collection create challenges for deploying comprehensive prevention strategies, and many institutions still underutilize tools that could improve detection accuracy. The growth of digital transactions has expanded opportunities for payments fraud, often linked to account takeovers, resulting in stolen funds or unauthorized purchases.

From a supply perspective, biometric authentication methods such as facial recognition are gaining prominence for secure logins and transaction approvals, offering both security and convenience. Passwordless authentication standards like FIDO2 remove the risks associated with traditional credentials. Continuous authentication methods provide ongoing identity verification during a user's session, and capabilities to detect social engineering scams are increasingly prioritized as attackers refine manipulation techniques. Together, these measures form the foundation of a layered defense strategy that can adapt to evolving threats.

Liminal's Use Case Methodology: Key Product Requirements

To effectively support ATO processes, vendors must fulfill five key product requirements, each encompassing a range of capabilities with varying levels of demand

Five key requirements outline the product capabilities and technical features needed to solve ATO. For a comprehensive mapping of these capabilities to corresponding technical features, please refer to **Link™**. The following scale was used to prioritize capabilities:

- **High:** Capabilities essential for solving the use case
- **Medium:** Helpful capabilities
- **Low:** Capabilities that practitioners do not prioritize

Requirements to Satisfy the Use Case		Buyer Demand for Product Capability[1]
Authenticate Customer Accounts	Verifies that a user accessing a system is the legitimate owner of the account. This typically involves validating identity credentials, such as passwords, multi-factor authentication (MFA), biometric data, or one-time passcodes, at the time of login or during sensitive transactions. The goal is to ensure only authorized users can access or modify account information, protecting against unauthorized access, fraud, and identity theft.	App-Based Authentication ● Multi-Factor Authentication (MFA) ● Biometric Authentication ◉ Continuous Authentication ◉ Adaptive Authentication ○ Passwordless Authentication ○
Detect Anomalous Behavioral Activity for Fraud Threats	Analyzes user behavior to identify actions that deviate from typical patterns and may indicate fraudulent intent. By detecting these anomalies in real time, organizations can flag potential first-party, third-party, or synthetic identity fraud before it results in financial loss.	Data Breach Monitoring ● Location Intelligence ● Behavioral Biometrics ◉ Device Health Status Detection ◉ SIM Swap Detection ◉ Social Engineering and Scam Detection ◉ Behavioral Analytics ○ Bot Detection ○
Detect Suspicious Transactions for Fraud	Analyzes transaction data for anomalies, patterns, and behaviors indicative of fraud. This capability involves monitoring transactions in real-time or near real-time using rule-based engines, machine learning models, or behavioral analytics to flag unusual activity, such as sudden changes in spending, high-risk geographies, or rapid movement of funds.	Behavioral Biometrics ◉ Fraud Monitoring ◉ Location Intelligence ◉ Behavioral Analytics ○
Enable Identity Self-Service Capabilities	Provides users with the tools to manage their own identity-related tasks, such as resetting passwords, updating personal information, or managing access permissions. This requirement enhances user experience by offering convenience and reducing the burden on IT support, while still maintaining security and compliance standards.	Customer Identity Self-Service capabilities ◉
Trigger Dynamic Authentication Based on User Risk	Adjusts the level of authentication required based on the perceived risk associated with a user's actions. This requirement enhances security by requiring additional verification steps, such as multi-factor authentication, when unusual or high-risk activities are detected.	Endpoint and Device Behavioral Analytics ● App-Based Authentication ◉ Behavioral Analytics ◉ Behavioral Biometrics ◉ Continuous Authentication ◉ Location Intelligence ◉ Multi-Factor Authentication (MFA) ◉ Adaptive Authentication ○ Passwordless Authentication ○

● High ◉ Medium ○ Low

1 Third Party Fraud Buyer Demand Survey, August 2025 (N=73)

ATO Buyer Personas

Chief Risk Officers, Chief Financial Officers, and Head of Fraud Prevention Drive Customer Service, Security, Fraud Mitigation, and Compliance Strategy

01

Chief Risk Officer

As the primary Decision Maker within the Risk department of a regional bank, this individual holds ultimate authority over the selection and approval of solutions addressing account takeover (ATO) fraud. Responsible for safeguarding customer accounts and the bank's reputation, they prioritize minimizing financial losses, ensuring regulatory compliance, and maintaining customer trust.

02

Chief Financial Officer

As a Champion within the Finance department of a multi-national bank, this individual is a proactive advocate for innovative solutions to combat Account Takeover (ATO) Fraud. Typically holding a senior finance or risk management role, they are responsible for safeguarding the institution's financial assets, ensuring regulatory compliance, and maintaining customer trust across diverse markets.

03

Head of Fraud Prevention

The Head of Fraud Prevention is responsible for developing and implementing strategies to detect, prevent, and mitigate fraud across the organization. This role oversees the deployment of fraud detection systems, monitors fraud trends, and collaborates with departments like IT, risk, and compliance to ensure a cohesive and effective approach to mitigating fraud risks across all business activities.

01 02 03

Chief Risk Officer

A Chief Risk Officer integrating ATO fraud detection reduces financial losses, strengthens regulatory compliance, and safeguards customer trust

As the Chief Risk Officer of a regional bank, this individual oversees all risk management functions, holding ultimate authority for selecting and approving solutions to prevent account takeover (ATO) fraud. They focus on minimizing financial loss, ensuring compliance, and maintaining customer trust by seeking scalable, data-driven tools that integrate effectively and demonstrate measurable impact on the bank's overall risk posture.

Goals

- Ensure Regulatory Compliance for Account Security
- Streamline Incident Detection and Response for Web Applications
- Facilitate Seamless Integration with Legacy and New Systems
- Enable Scalable and Maintainable Account Security Solutions
- Balance Customer Experience with Security Controls
- Minimize Fraud and Protect Customer Assets
- Enable Dynamic User and Entity Risk Scoring
- Demonstrate ROI and Cost-Effectiveness of Anti-Abuse Solutions
- Support Dynamic Context-Aware Authentication and Authorization

Frustrations

- Inadequate Real-Time Dynamic Risk Scoring
- Limited Customization and Scalability for Regional Bank Needs
- Staff Training and Adoption Challenges
- Difficulty Quantifying and Demonstrating ROI for Fraud Prevention Investments
- Vendor Expertise and Support Gaps in AI Data Governance
- Evolving Account Sharing and Fraud Tactics
- Balancing Security with User Experience
- Resource Constraints
- Integration Challenges with Existing Banking Systems

KPCs

- Ease of Implementation
- Accuracy
- Pricing
- Data Quality
- Internal User Experience
- Analytical Capabilities
- Scalability
- End-Customer Experience
- Compliance Alignment
- Automation

01 02 03

Chief Financial Officer

A Chief Financial Officer advancing ATO prevention enforces financial resilience, strengthens compliance oversight, and safeguards institutional integrity

The Chief Financial Officer (CFO) serves as a key decision-maker and advocate for fraud prevention within the finance function, prioritizing financial integrity, regulatory compliance, and operational resilience across markets. They evaluate and implement scalable, data-driven solutions that mitigate Account Takeover (ATO) fraud while ensuring alignment with risk frameworks, cost efficiency, and customer trust objectives.

Goals

- Ensure Data Security and Privacy in KYC Processes
- Enable Scalable and Maintainable Account Security Solutions
- Continuously Monitor and Detect Anomalous User Behavior
- Authenticate and Secure Customer Accounts
- Integrate Fraud Prevention Solutions with Existing IT Infrastructure
- Minimize Fraud and Protect Customer Assets
- Enable Dynamic User and Entity Risk Scoring
- Enable Dynamic Risk-Based Authentication
- Demonstrate ROI and Cost-Effectiveness of Anti-Abuse Solutions

Frustrations

- Vendor Transparency and Data Handling Concerns
- Insufficient Support for Global Scalability
- Unclear ROI and Cost Justification
- Insufficient Anomalous Activity Detection
- Lack of Real-Time Regulatory Risk Dashboards
- Rapid Evolution of ATO Fraud Tactics Across Geographies
- Balancing Security with User Experience
- Limited Customization of ATO Solutions for Operational Needs
- Integration Challenges with Legacy and Diverse Systems

KPCs

- Compliance Alignment
- Accuracy
- Data Quality
- Pricing
- Analytical Capabilities
- Automation
- Scalability
- Ease of Implementation
- Internal User Experience
- End-Customer Experience

01 02 03

Head of Fraud Prevention

A Head of Fraud Prevention implementing ATO fraud strategies reduces false positives, strengthens threat detection, and safeguards customer accounts

The Head of Fraud Prevention is responsible for leading the development and execution of strategies to prevent and mitigate account takeover (ATO) fraud within the organization. This role oversees the implementation of fraud detection systems, monitors account activity for suspicious behavior, and collaborates with security, IT, and customer service teams to ensure effective prevention and response to ATO threats, safeguarding customer accounts and reducing fraud losses.

Goals

- Ensure Regulatory Compliance for Account Security
- Reduce False Positives in Authentication Processes
- Enable Cost-Effective and Scalable ATO Fraud Prevention
- Minimize Customer Friction While Maintaining Security
- Demonstrate ROI and Cost-Effectiveness of Anti-Abuse Solutions
- Enable Dynamic User and Entity Risk Scoring
- Enable Dynamic Risk-Based Authentication
- Enable Comprehensive, Real-Time Security Monitoring
- Maintain and Strengthen Customer Trust and Bank Reputation

Frustrations

- Inadequate Real-Time Dynamic Risk Scoring
- Limited Customization and Scalability for Regional Bank Needs
- Evolving and Sophisticated Fraud Tactics
- Unclear ROI and Cost Justification
- Resource Constraints for Technology Adoption
- Balancing Security with User Experience
- Overwhelming Volume of Alerts and False Positives
- Integration Challenges with Legacy and Heterogeneous Systems

KPCs

- Ease of Implementation
- Accuracy
- Pricing
- Data Quality
- Internal User Experience
- Analytical Capabilities
- Scalability
- End-Customer Experience
- Compliance Alignment
- Automation

End-to-End Solutions Prevent ATO, Detect Fraud, and Protect Banks From ATO Exploitation

1 User Accesses Online Banking Portal - Entering the Online Banking Portal

When a user accesses the online banking portal, the security platform begins collecting behavioral signals that can be tracked and analyzed. These signals include geolocation, IP address, device information (e.g., type of device, operating system), and keystroke dynamics. Additional data points such as mouse movements, screen touches, and navigation patterns are also collected. This enables the platform to continuously monitor the user's behavior to detect any anomalies that may indicate fraudulent activity.

2 User Attempts Login - Initiating Login Process

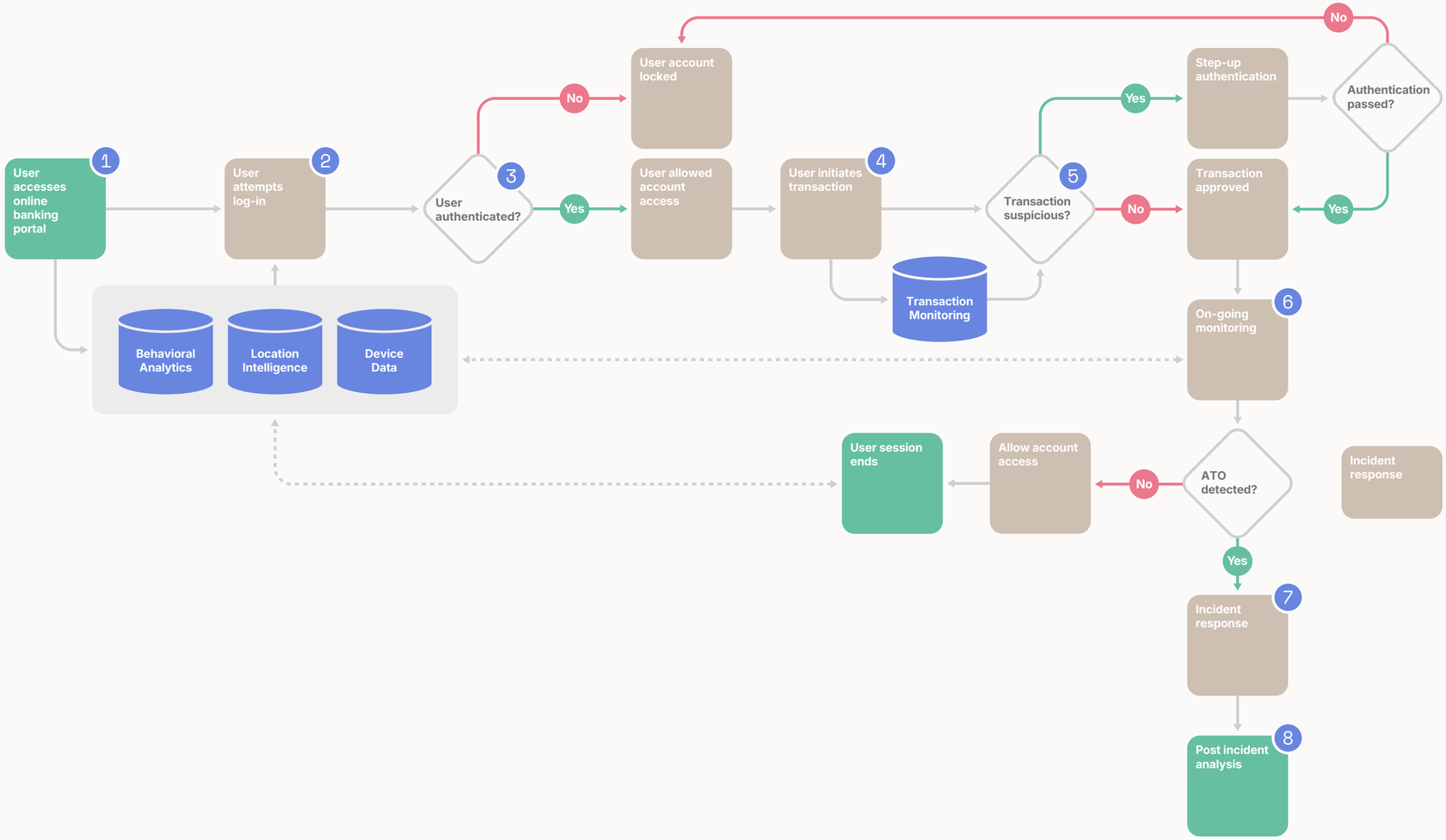
During the login attempt, the security platform analyzes the user's credentials, IP address, device characteristics, and behavioral biometrics. This includes typing speed, keystroke patterns, and mouse movements. The platform compares these behaviors against the user's historical patterns to identify any deviations that may signal an account takeover attempt. Multi-factor authentication (MFA) is prompted for additional verification if anomalies are detected.

3 User is Authenticated - Successful or Unsuccessful Authentication

Upon authentication, the platform evaluates the success or failure of the login attempt. If the login is successful but suspicious behavior is detected, the user may be required to complete additional verification steps, such as answering security questions or performing a biometric verification. For unsuccessful attempts, the account may be temporarily locked after a set number of failed attempts, and the user is alerted via email or SMS about the suspicious activity.

4 User Initiates Sensitive Transaction - Transaction Initiation

When the user initiates a sensitive transaction, such as a funds transfer or bill payment, the security platform analyzes the transaction in real-time. It considers the transaction amount, destination, frequency, and historical user behavior. Behavioral biometrics continue to be monitored to detect any anomalies during the transaction process. Any deviations from the user's typical behavior or transaction patterns trigger an additional security review.



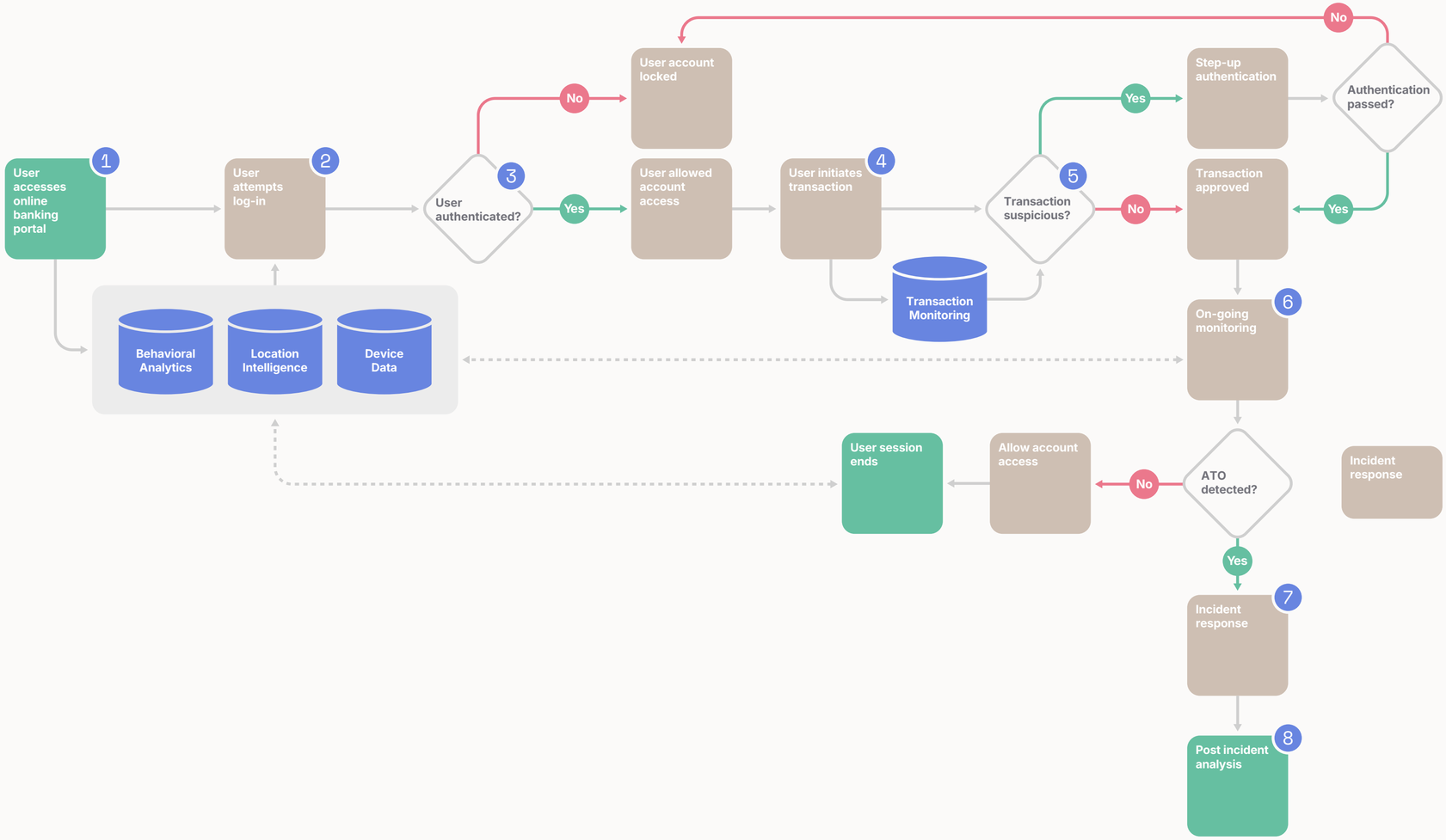
5 Transaction Verification - Real-Time Risk Assessment
The platform performs a real-time risk assessment of the transaction, utilizing machine learning models and behavioral analytics. If the transaction is deemed high-risk, the user is prompted to verify their identity through MFA or other verification methods. The platform may also use adaptive authentication techniques, adjusting the security requirements based on the assessed risk level.

6 Continuous Monitoring - Ongoing Behavioral Analysis
Even after successful authentication and transaction approval, the platform continues to monitor the user's session for any signs of suspicious activity. This includes monitoring for unusual navigation patterns, sudden changes in geolocation, or atypical device usage. Continuous monitoring helps in detecting and mitigating any ongoing account takeover attempts.

7 Incident Response - Handling Detected Threats
If an account takeover attempt is detected, the platform triggers an incident response protocol. This includes alerting the user, locking the account, and initiating an investigation. The user is guided through account recovery steps, such as resetting passwords and updating security settings. The platform also logs detailed information about the incident for further analysis and improvement of security measures.

8 Post-Incident Analysis - Learning and Improvement
After an incident, a thorough analysis is conducted to understand how the account takeover attempt occurred and to identify any gaps in the security measures. The insights gained are used to improve the platform's detection algorithms and response protocols. Regular updates and training are provided to both the security team and customers to enhance overall security awareness and resilience.

End-to-End Solutions Prevent ATO, Detect Fraud, and Protect Banks From ATO Exploitation







02

Market Overview

ATO Key Insights

Organizations face a wide range of threats, from credential stuffing and phishing to SIM swap fraud, straining already overextended teams

95%

95% of practitioners observe continuous attempts against the same compromised accounts, highlighting repeat victimization as a significant challenge in fraud prevention

Fragmented Threat Landscape Forces Organizations to Defend Against Multiple Attack Vectors

Organizations confront a multifaceted threat landscape, lacking a single dominant attack vector. Credential stuffing, social engineering, and man-in-the-middle attacks each represent significant threats, contributing 27%, 26%, and 26% respectively. Additionally, SIM swap fraud (21%) and phishing (19%) further compound the challenges. This broad spectrum of threats makes it difficult for organizations to allocate resources effectively, often leaving security teams overextended as they attempt to address diverse risks simultaneously.[1]

Persistent Attacks on Compromised Accounts Highlight Ongoing Exposure to Repeat Targeting

A significant challenge in fraud prevention is repeat victimization, with 95% of practitioners observing continuous attempts against the same compromised accounts. The exposure of an account frequently leads to its becoming a persistent target, suggesting that initial breaches create enduring vulnerabilities. This ongoing threat necessitates that organizations enhance their defenses beyond single-instance detection, implementing sustained protection strategies.[1]

Rising Mobile Vulnerabilities Increase Pressure on Organizations to Invest in Fraud Protection

Mobile channels face a higher risk of attacks, with incidents 2.5 times more frequent than on desktop. This increased vulnerability in mobile apps and browsers is attributed to the difficulty in managing security loopholes. Consequently, 78% of professionals expect to boost their investment in mobile fraud prevention within the next two years, indicating its critical role in future strategies. Alongside mobile, professionals also expect rising threats across third-party partners (76.7%), API integrations (74%), desktop (69.9%), and call centers (65.8%), underscoring the need for broad and proactive defenses.[1]

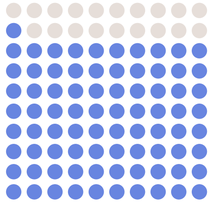
Fragmented Team Ownership and Coordination Gaps Undermine Effective Threat Response Efforts

Poor coordination and unclear ownership across teams pose significant challenges to effective incident response, largely due to organizational silos. While IT security handles 78% of prevention efforts, 69% of practitioners report that ambiguous ownership slows down decisions and response times. This lack of formal planning and fragmented accountability is a major concern, cited twice as often as issues like customer churn or delayed resolution, highlighting its substantial cost.[1]

1 Third Party Fraud Buyer Demand Survey, August 2025 (N=73)

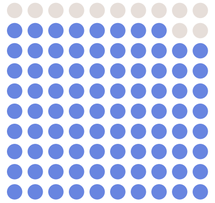
ATO Operational Barriers

Organizations adopt automated re-verification at scale, reducing manual reviews and reinforcing recovery as central to fraud strategy



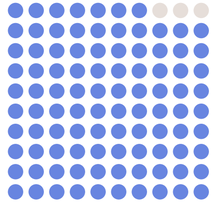
81%

of practitioners favor automated identity re-verification methods in recovery processes



88%

of practitioners admit to not prioritizing stronger safeguards due to concerns about user friction and abandonment



97%

of practitioners confirm authentication's ability to reduce risk exposure, and it is widely recognized as a highly effective defense mechanism

Growing Reliance on Authentication Underscores Demand for Stronger Identity Protection Measures

Authentication is widely recognized as a highly effective defense mechanism, with 97% of practitioners confirming its ability to reduce risk exposure. This strong consensus indicates a significant demand for authentication-based solutions that offer dependable protection across various environments. Consequently, organizations are increasingly prioritizing these measures, establishing authentication as a fundamental element of their prevention strategies.[1]

Escalating Need for Automated Recovery Highlights Demand for Scalable Identity Re-Verification

Automated identity re-verification methods are now favored by 81% of practitioners in recovery processes, compared to only 21% who still rely on manual case reviews. This shift emphasizes the demand for scalable workflows that reduce dependency on resource-intensive approaches and enable more consistent recovery outcomes. Importantly, 95% of practitioners consider post-breach ATO prevention and recovery a central element of their fraud strategy, further reinforcing the need for reliable re-verification at scale.[1]

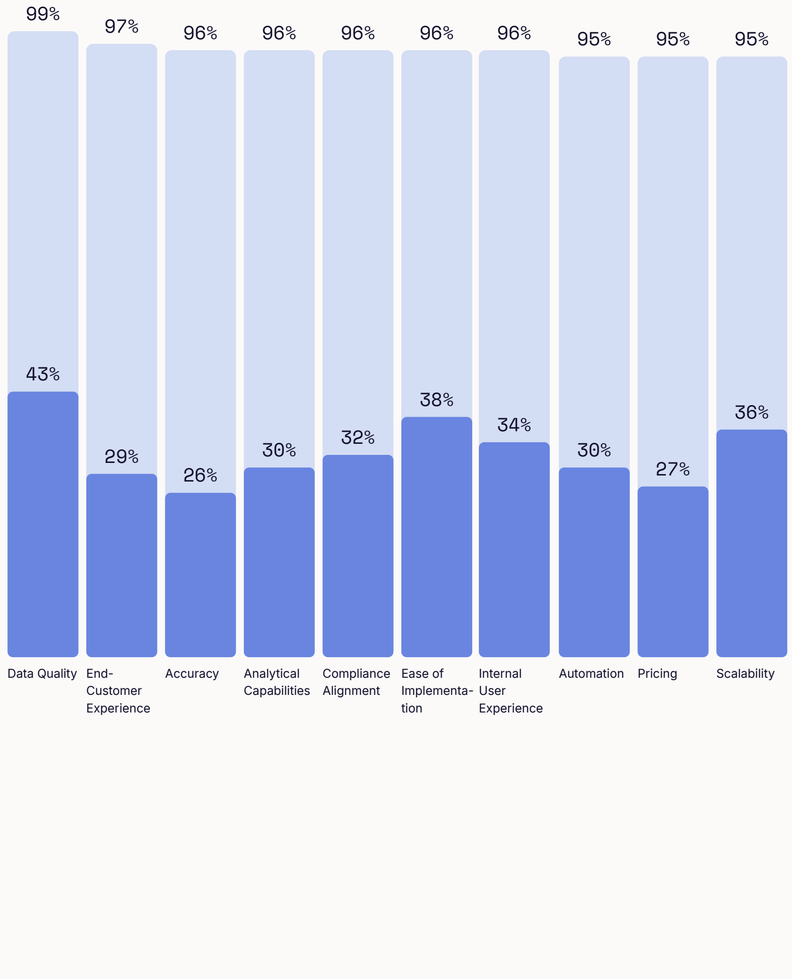
Demand Grows for Frictionless Recovery Balancing Security With Customer Retention Priorities

Organizations express varied levels of confidence in the strength of recovery, with 42% of practitioners finding their current processes ineffective, 5% neutral, and 52% effective. Despite acknowledging security risks, 88% admit to not prioritizing stronger safeguards due to concerns about friction and abandonment. At the same time, 61% report that their ATO response plan improved customer trust and satisfaction. These findings highlight the need for recovery solutions that provide both seamless experiences and strong protection.[1]

1 Third Party Fraud Buyer Demand Survey, August 2025 (N=73)

Key Purchasing Criteria for ATO Solutions[1]

ATO practitioners prioritize data quality and end-customer experience as the most important criteria in their purchasing process



1 Third Party Fraud Buyer Demand Survey, August 2025 (N=73)

ATO Future Outlook

The market is preparing layered defenses against AI-driven risks, while buyers prioritize unified platforms and third-party protections

80%



of practitioners anticipate increasing investments in fraud prevention specifically targeting partner channels

88%



of practitioners prefer one-stop platforms or orchestration layers, showing that buyers are increasingly seeking integrated solutions

96%



of practitioners identifying generative AI as an escalating risk

Escalating Multi-Vector Risks Drive Demand for Layered Defenses and AI-Adapted Detection

Organizations confront continuous exposure to threats from various attack vectors, necessitating layered defenses. The concern is underscored by 96% of practitioners identifying generative AI as an escalating risk. In response, 66% expect to increase model tuning and signal diversity and 34% plan to invest in new detection techniques—together representing 100% of practitioners preparing to counter AI-driven attacks.[1]

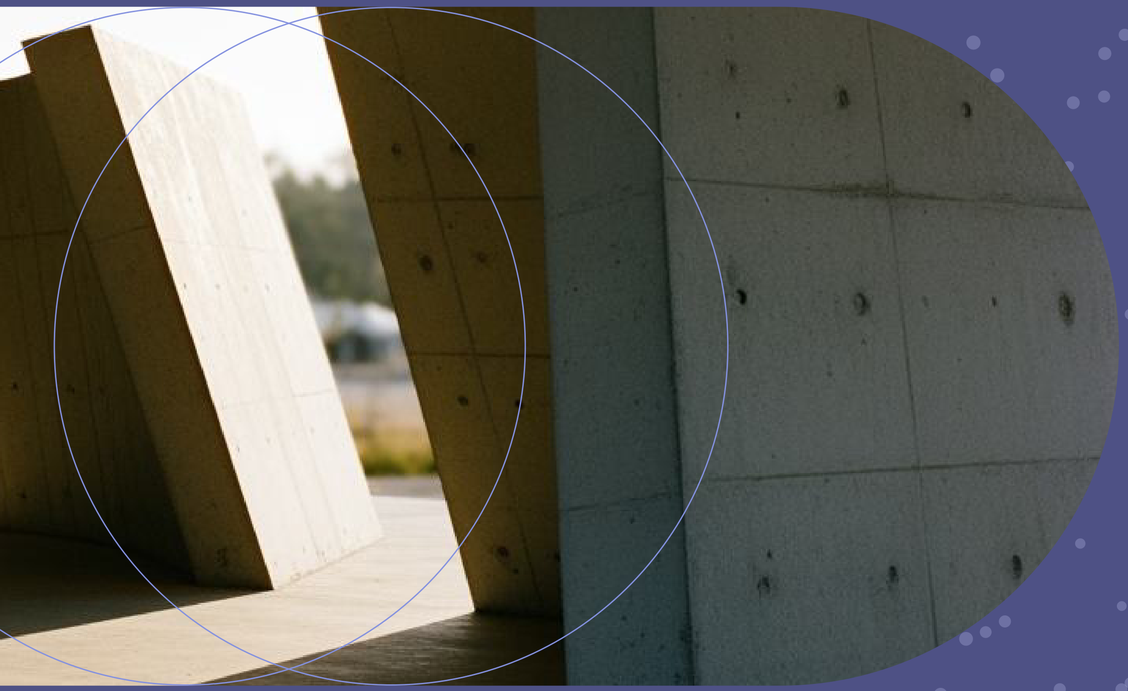
Focus on Third-Party Channels Signals Anticipated Investment in Partner Risk Controls

While only 7% of practitioners identified third-party partners as the primary risk in the past year, expectations are changing. Over the next two years, 80% anticipate increasing investments in fraud prevention specifically targeting partner channels. This shift indicates a growing awareness that, despite not currently being the biggest threat, third-party ecosystems require proactive protective measures.[1]

Preference for Unified Platforms and Orchestration to Simplify Threat Mitigation Efforts

Buyers are increasingly seeking integrated solutions, with 88% of practitioners preferring one-stop platforms or orchestration layers. This indicates a strong demand for consolidated ecosystems that optimize operations and strengthen security, whether through comprehensive platforms for various fraud use cases or orchestration models connecting third-party vendors. Yet, the practicality of consolidation is limited; organizations anticipate their number of ATO vendors to rise slightly (6%) in the next 12 months, suggesting stacks will remain diversified despite platform preference.[1]

1 Third Party Fraud Buyer Demand Survey, August 2025 (N=73)



03

Link Index



ATO Vendor Product Evaluation

Vendor products were evaluated based on their coverage of product capabilities and performance against top solution purchasing criteria

Additional Factors for Consideration

Buyer Satisfaction	The extent of buyer satisfaction with a vendor's solution.
Generative AI Guardrails	Evaluates defenses against AI-driven ATO threats, including manipulated content and synthetic identities.
Data Quality & Integrity	Reviews the accuracy, completeness, and timeliness of account, transaction, and identity data used for ATO detection and response.
Post-ATO Recovery Process	Examines mechanisms for user re-entry and remediation following a confirmed ATO incident.
Authentication Flow Adaptability	Assesses how dynamic and context-aware authentication methods are in mitigating ATO risk. Goes beyond basic MFA to adaptive, risk-based flows.

● High ◉ Medium ○ Low

1 Third Party Fraud Buyer Demand Survey, August 2025 (N=73)

Requirements to Satisfy the Use Case		Buyer Demand for Product Capability[1]
Authenticate Customer Accounts	Verifies that a user accessing a system is the legitimate owner of the account. This typically involves validating identity credentials, such as passwords, multi-factor authentication (MFA), biometric data, or one-time passcodes, at the time of login or during sensitive transactions. The goal is to ensure only authorized users can access or modify account information, protecting against unauthorized access, fraud, and identity theft.	App-Based Authentication ● Multi-Factor Authentication (MFA) ● Biometric Authentication ◉ Continuous Authentication ◉ Adaptive Authentication ○ Passwordless Authentication ○
Detect Anomalous Behavioral Activity for Fraud Threats	Analyzes user behavior to identify actions that deviate from typical patterns and may indicate fraudulent intent. By detecting these anomalies in real time, organizations can flag potential first-party, third-party, or synthetic identity fraud before it results in financial loss.	Data Breach Monitoring ● Location Intelligence ● Behavioral Biometrics ◉ Device Health Status Detection ◉ SIM Swap Detection ◉ Social Engineering and Scam Detection ◉ Behavioral Analytics ○ Bot Detection ○
Detect Suspicious Transactions for Fraud	Analyzes transaction data for anomalies, patterns, and behaviors indicative of fraud. This capability involves monitoring transactions in real-time or near real-time using rule-based engines, machine learning models, or behavioral analytics to flag unusual activity, such as sudden changes in spending, high-risk geographies, or rapid movement of funds.	Behavioral Biometrics ◉ Fraud Monitoring ◉ Location Intelligence ◉ Behavioral Analytics ○
Enable Identity Self-Service Capabilities	Provides users with the tools to manage their own identity-related tasks, such as resetting passwords, updating personal information, or managing access permissions. This requirement enhances user experience by offering convenience and reducing the burden on IT support, while still maintaining security and compliance standards.	Customer Identity Self-Service capabilities ◉
Trigger Dynamic Authentication Based on User Risk	Adjusts the level of authentication required based on the perceived risk associated with a user's actions. This requirement enhances security by requiring additional verification steps, such as multi-factor authentication, when unusual or high-risk activities are detected.	Endpoint and Device Behavioral Analytics ● App-Based Authentication ◉ Behavioral Analytics ◉ Behavioral Biometrics ◉ Continuous Authentication ◉ Location Intelligence ◉ Multi-Factor Authentication (MFA) ◉ Adaptive Authentication ○ Passwordless Authentication ○

ATO Vendor Strategy Evaluation

ATO vendor strategies were assessed based on the top buyer purchasing priorities for the coming years

01

Ease of Implementation

Assesses the level of effort required to deploy the solution across key systems such as payment gateways, CRMs, and fraud platforms. Prebuilt integrations and streamlined onboarding reduce deployment complexity and shorten time to value.

02

End-Customer Experience

Measures the solution's ability to protect accounts without creating friction for legitimate users. A consistent and fair experience strengthens customer trust and reduces abandonment.

03

Scalability

Evaluates the solution's capacity to support increasing transaction volumes and adapt to evolving fraud tactics. Scalable solutions maintain performance and accuracy as customer bases and attack surfaces expand.

04

Orchestration / Platform Approach

Reviews whether the solution functions as a broader platform versus a single-point tool. Platforms provide unified coverage across multiple fraud and identity use cases, while orchestration allows integration with third-party vendors.

ATO Vendor Market Presence Evaluation

The market presence of ATO vendors was evaluated based on company size and growth, leadership perception, funding, digital footprint, and media coverage



Company Size

This criterion measures a vendor's total workforce to indicate its operational capacity, available resources, and scalability. In the identity verification sector, a larger company size often corresponds to greater infrastructure, regulatory expertise, and client support capabilities, reflecting an organization's ability to sustain and evolve its service delivery.



Employee Growth (YoY)

This criterion tracks the year-over-year change in a vendor's workforce, signaling organizational expansion and investment in capability areas such as compliance, technology development, and customer support. Sustained growth can indicate rising demand for solutions and the vendor's capacity to scale operations to meet evolving client requirements.



Market Leadership Perception

This criterion captures how the market perceives a vendor's leadership within the identity verification landscape, including its innovation, reliability, and influence. A strong leadership perception suggests trust in the vendor's solutions, the ability to shape industry standards, and recognition as a preferred partner for compliance and verification initiatives.



Funding History

This criterion assesses the vendor's financial backing, including the volume, frequency, and sources of external investment. A strong funding record demonstrates market confidence, provides resources for innovation and expansion, and supports long-term stability within the identity verification ecosystem.



Digital Footprint

This criterion evaluates the extent and quality of a vendor's digital presence, including its website performance, social engagement, and online visibility. A strong digital footprint indicates active market communication, accessibility to buyers, and transparency about product capabilities and compliance posture.

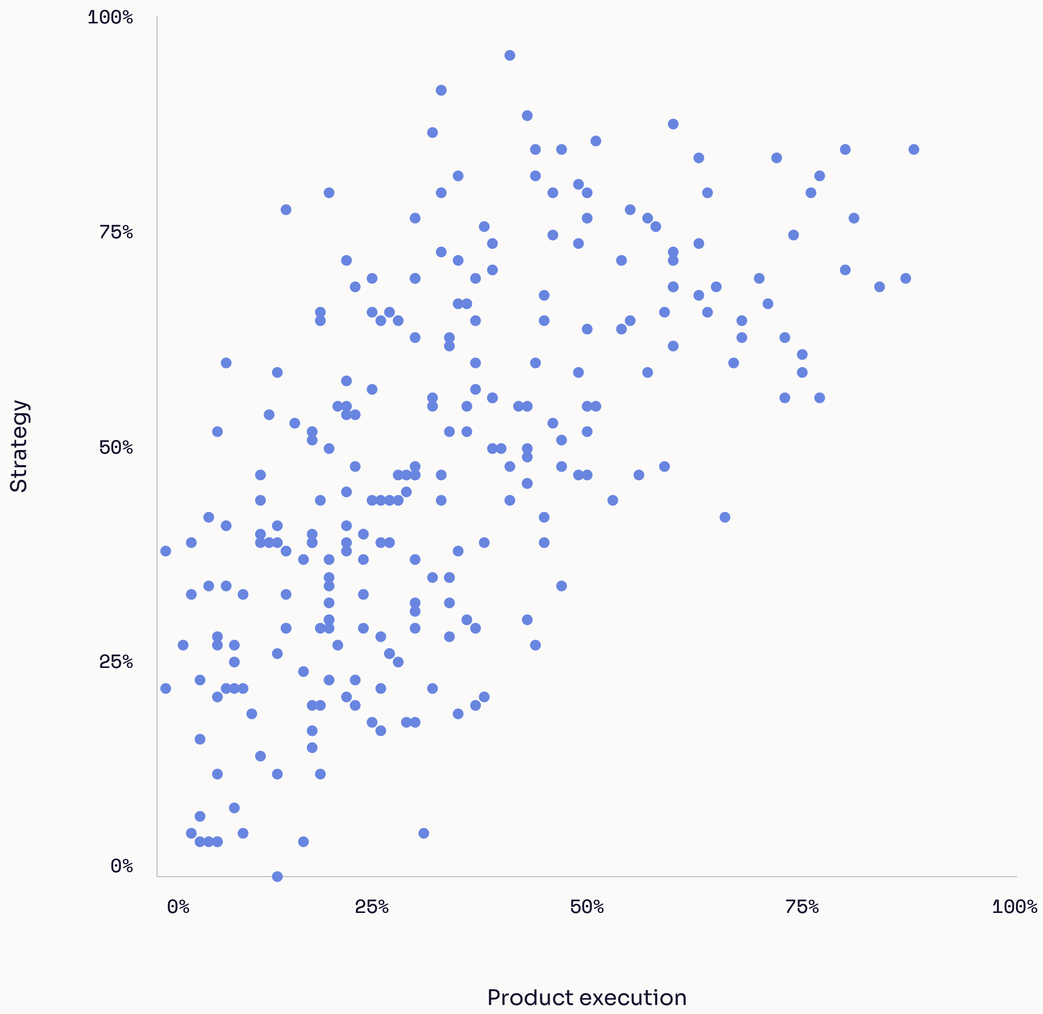


Media Coverage

This criterion measures the volume and sentiment of media mentions related to the vendor across industry and mainstream sources. Consistent, positive coverage reflects market relevance, public trust, and influence, while high visibility across credible outlets can signal leadership and authority in the identity verification space.

ATO Vendor Evaluation

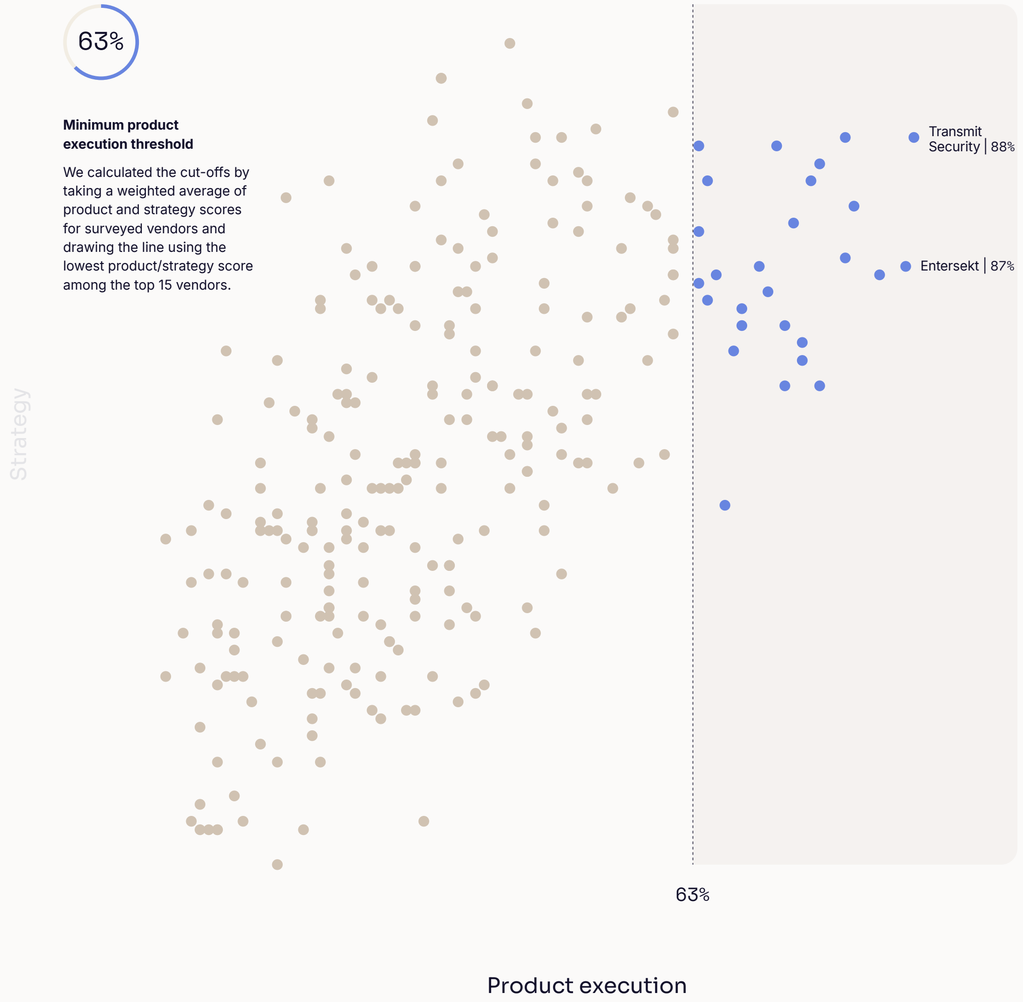
Liminal evaluated 258 vendors that solve the Account Takeover Prevention in Banking use case. Minimum product execution and strategy thresholds were established to identify the leading vendors



Leadership Thresholds for ATO

Minimum product execution threshold

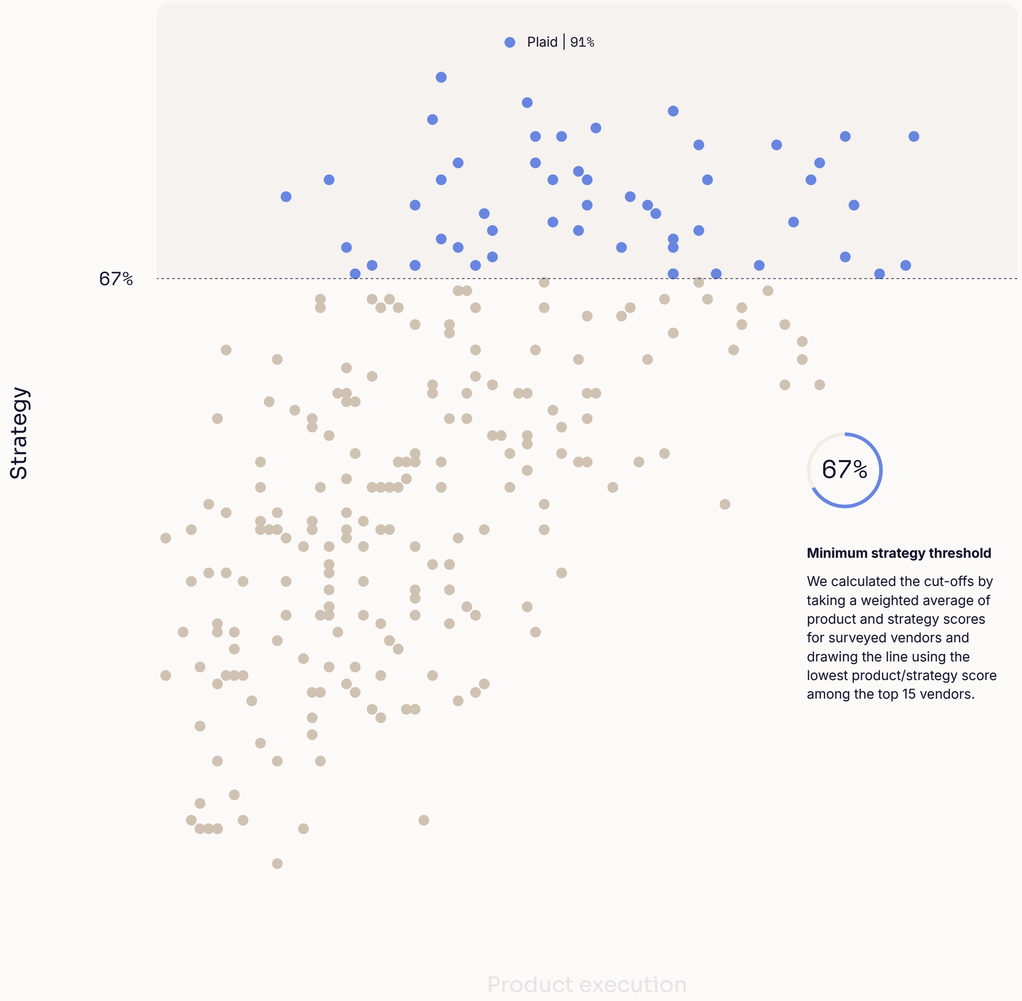
To establish a minimum product execution threshold for ATO prevention, we evaluated practitioner feedback and buyer demand across the banking and financial services sectors. The highest-value product capabilities identified include detection accuracy, data quality, authentication adaptability, orchestration capabilities, and end-customer experience. These capabilities collectively define a vendor's ability to detect and mitigate unauthorized access while maintaining low friction for legitimate users. Based on aggregated buyer demand and solution performance benchmarks, vendors must achieve a minimum product execution score of 63% to sufficiently meet the requirements of a leading ATO prevention solution.



Leadership Thresholds for ATO

Minimum strategy threshold

The strategy threshold for ATO prevention reflects the market's shift toward layered, AI-adapted defenses and unified fraud management platforms. Key elements driving strategic differentiation include scalability, automation, orchestration, integration with existing fraud and identity systems, and resilience against generative AI threats. Vendors must also demonstrate a forward-looking investment strategy emphasizing continuous model tuning, post-ATO recovery, and proactive protection against emerging attack vectors. To qualify as a strategic leader in ATO prevention, a vendor must achieve a minimum strategy score of 67%, signaling alignment with evolving buyer expectations for platform consolidation, adaptive authentication, and AI-driven fraud detection frameworks.

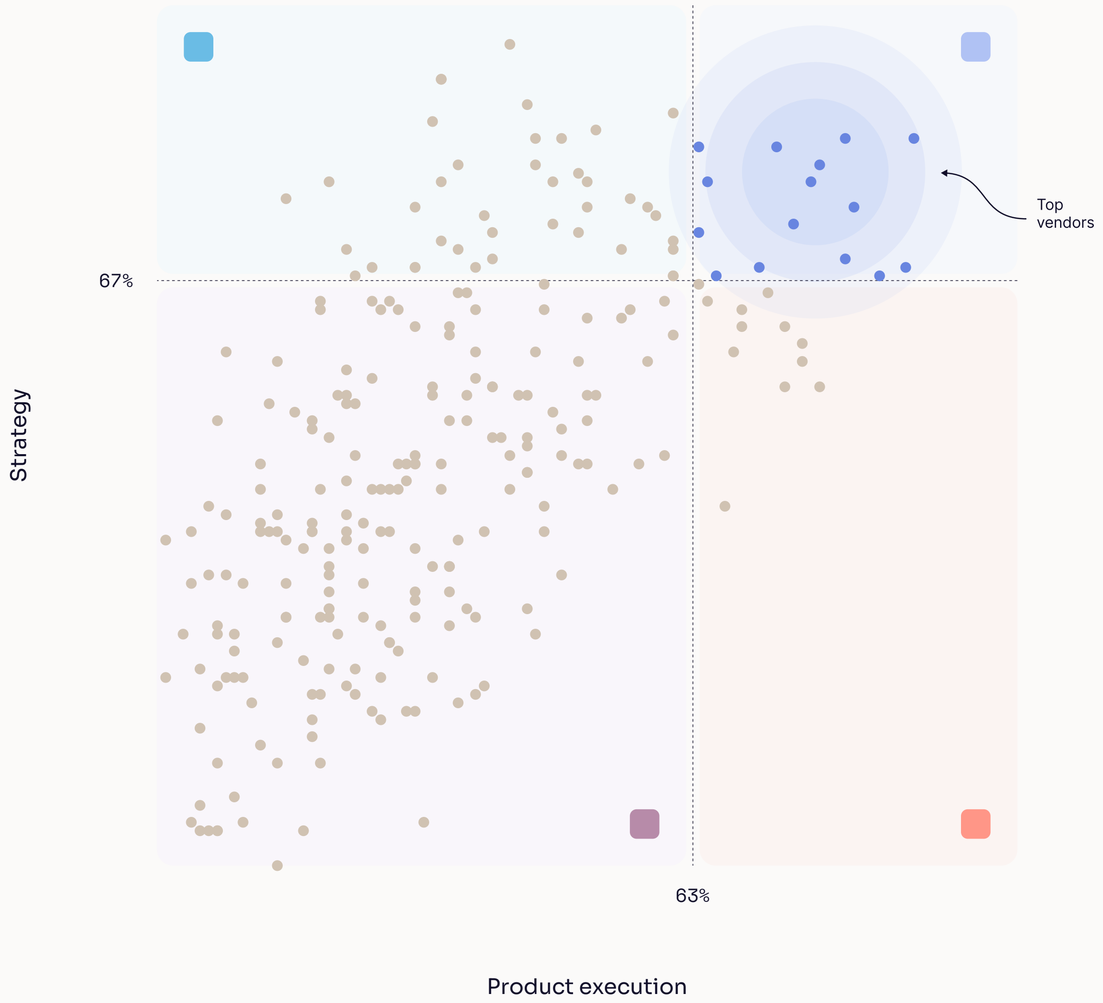


Minimum strategy threshold

We calculated the cut-offs by taking a weighted average of product and strategy scores for surveyed vendors and drawing the line using the lowest product/strategy score among the top 15 vendors.

ATO Leading Vendors

Among the 258 vendors Liminal evaluated that solve the Account Takeover Prevention in Banking use case, 15 leading vendors met the minimum product and strategy threshold



Adjacent Vendors
Strong overall solutions but do not have the required capabilities for this use case

Leading Vendors
Strong overall solutions that possess the must have product and strategy capabilities for this use case

Specialized Vendors
Solutions that can solve for a part of the use case but do not have all must have capabilities

Product-Focused Vendors
Solutions with strong product capabilities but do not meet the strategy score threshold

Liminal

15 Leaders, 258 Evaluated Vendors

Liminal evaluated 258 vendors that solve the Account Takeover Prevention in Banking use case across the product and strategy criteria, and determined 15 leading vendors

Leaders

AppGate
BioCatch
Callsign
Datavisor
Descope
Entersekt
Equifax (Kount)
Experian
Incode
LexisNexis Risk Solutions
Ping Identity
Prove
Sumsub
Transmit Security
TransUnion

Other Evaluated Vendors

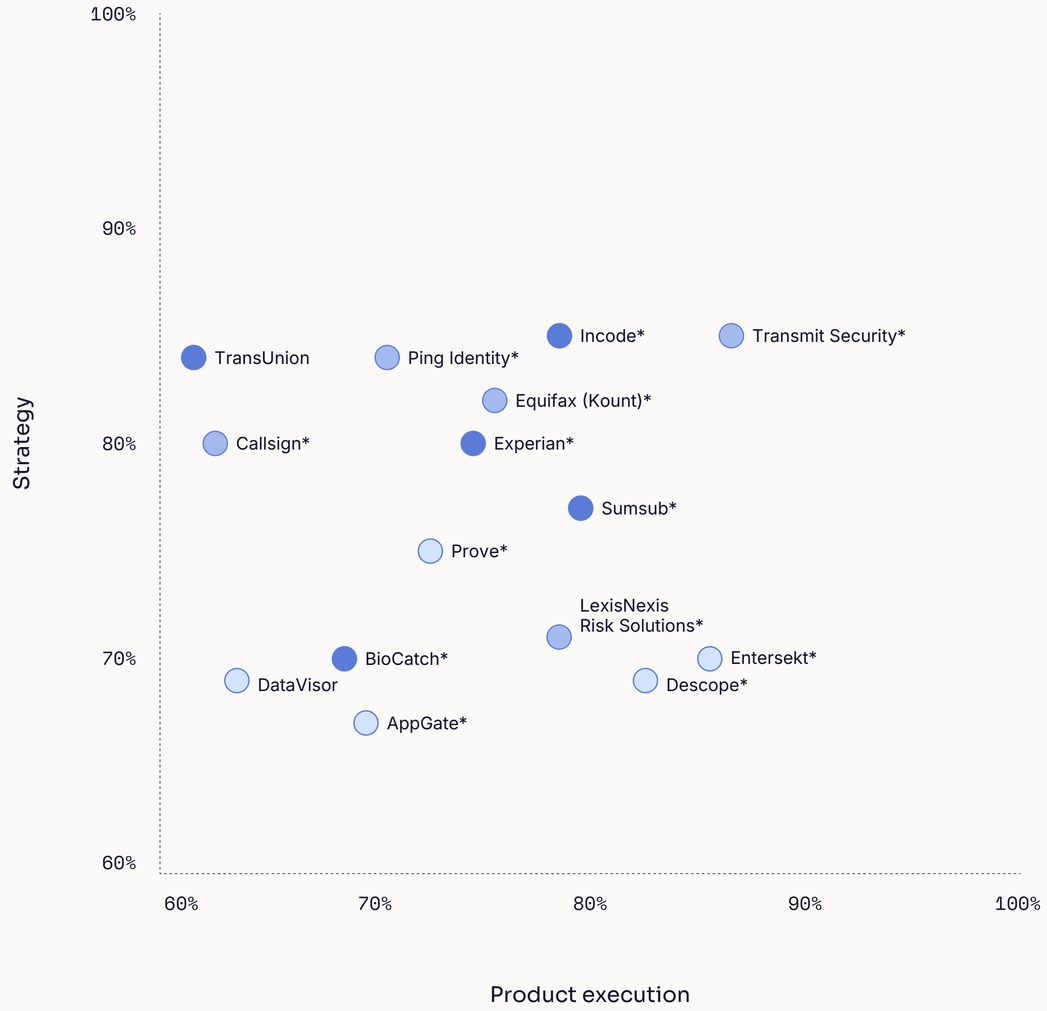
Adjacent Vendors
1Kosmos
Bureau
CrossClassify
Darwinium
DataDome
Dojah
Enzoic
FICO
FIS
Fiserv
fraud.com
GBG
Group-IB
HID Global
HyperVerge
ID Dataweb
Infobip
IPQualityScore
Ironchip
Jack Henry
Jumio
Mangopay
Mastercard
MEMCYCO
NICE Actimize
Nametag
OneSpan
Persona
Plaid
Q2
Radware
RSA Security
SAS
SEON
Signicat
Strivacity
TELUS Digital
Unit21
Veridium
Visa
Wallarm
Worldline

Product-Focused
Authsignal
Entrust
Feedzai
Footprint
Fraud.net
Outseer
Shufti
Socure
Veriff
Verosint

Specialized Vendors
1datapipe
4Stop
8x8
ABnormal AI
ACI Worldwide
ACSiON
ADVANCE.AI
Advanced Fraud Solutions
Accertify
Akamai Technologies
Alacer
Alessa
Alloy
Alphacomm
Amazon Web Services (AWS)
Anonybit
Appdome
Arkose Labs
Ascend Technologies
AtData
Banyan Software
Bayonet
BlueVoyant
BRANDEFENSE
Bynn
Caf
Castle
Celusion
Cisco Duo
Cleafy
Clari5
ComplyAdvantage
Complytek
Computer Services (CSI)
Constella Intelligence
Covery AI
Cursor Insight
Cyrus
Cyberint
CyberSiARA
Cybertonica
CybelAngel
DataSeers
Darktrace
Defendify
DefenseStorm
Deduce
DeviceAtlas
Didit
Dodgeball
Drona Pay
Enformion
EnStream
Escalated.io
EVS
FiVerity
Fingerprint
Flashpoint
Flare
Forter
Fortinet
Formica AI
FraudHunt
Fraudlogix
Fraudnetic
Fraugster
GeoComply
GeeTest
GBG
Grab
Graphus
GreatHorn
GuardianKey
Guardz
Gueno
HUMAN Security
hCaptcha
IBM
ID Watchdog
Identity Guard
IDSeal
IDScan.net
IDStrong
IDMERIT
iiDENTIFii
Immue
Infinipoint
INETCO
Incognia
INFORM
Intel 471
IronVest
JuicyScore
Kasada
Kevari
KELA
Keyless
Kiteworks
Linkurious
LogMeOnce
Lynx
Malwarebytes
Manipal Technologies Limited
McAfee
MiniAILive
MojoAuth
Monnai
Nametag
Nasdaq Verafin
neoEYED
Nevis Security
Netacea
NetNumber
nextAuth
Nord Security
Notolytix
Oneytrust
Oscilar
Palo Alto Networks
Paygilant
Pelican
Perfios
Permiso Security
Pindrop
Pipl
Plum Identity
Preventor
Proximus Global
Proofpoint
Protectt.ai
Push Security
Qrator Labs
Q6 Cyber
RangersAI
RaptorX.ai
Ravelin
RavenMail
Recorded Future
Refine Intelligence
Resecurity
Resistant AI
RevenueStream
Reveal Security
Riskified
Rupt
S2W
Saffe
Sardine
Scoria Labs
Scrub.io
Scriptr AI
SensFRX
Shadowbyte
SHIELD
Sign3
Signifyd
Sift
Simplici
Smartnumbers
Spec
Spikerz
Spycloud
SymphonyAI
Syniverse
Tirreno
TMT ID
Temenos
ThreatFabric
ThreatMark
Token of Trust
Tookitaki
Trend Micro
TrustDecision
Trustifi
Trustfull
TruSense
Trusona
Twilio
Uniken
Variti
Veracity Trust Network
Verisoul
VerifiedVisitors
Webz.io
Worldpay
XTN Cognitive Security
Yoti
Zander Insurance
ZeroFox
ZOLOZ
Zumigo

Link Index Leading Vendors for Account Takeover Prevention in Banking in 2025

This view includes the product and strategy score cut-off, showcasing the 15 Leading Vendors for this year's Account Takeover in Banking Index



Market Presence

- Exceptional
- Excellent
- Strong

Inclusion Cutoff

Product Score 63%
Strategy Score 67%

We calculated the cut-offs by taking a weighted average of product and strategy scores for surveyed vendors and drawing the line using the lowest product/strategy score among the top 15 vendors.

Companies with an asterisk (*) participated in an Analyst Briefing with Liminal for this report.

ATO Leading Vendor Characteristics

ATO vendors differentiate based on authentication depth, behavioral intelligence, and orchestration maturity

01

End-to-End Fraud and Risk Platforms

These vendors provide comprehensive coverage across fraud prevention, identity verification, and transaction risk management. Their platforms integrate behavioral analytics, authentication orchestration, and AI-driven anomaly detection to protect against ATO and related fraud schemes. They are commonly deployed by large financial institutions seeking unified fraud management frameworks that align with enterprise compliance and scalability requirements.

02

Authentication and Access Management Platforms

These platforms focus on securing user access and session integrity through adaptive authentication, continuous risk assessment, and multi-factor authentication (MFA). They specialize in reducing credential-based fraud by dynamically adjusting authentication levels based on user behavior, device health, and contextual risk indicators. Their solutions are particularly effective for institutions prioritizing secure, low-friction user experiences.

03

Behavioral and Device Intelligence Specialists

These vendors specialize in behavioral biometrics, device fingerprinting, and network analytics to detect anomalous activity that signals account compromise. They analyze interaction patterns, geolocation data, and device consistency to identify potential takeovers in real time. Their core strength lies in precision threat detection and integration flexibility, supporting use cases across digital banking, payments, and eCommerce.

ATO Leading Vendor Future Outlook

Leading vendors are shaping the future of ATO prevention through adaptive authentication, behavioral intelligence, and AI-driven defense

Adaptive, Low-Friction Authentication

Leading ATO vendors are redefining account security with adaptive authentication models that strengthen protection without increasing user friction. These solutions employ risk-based authentication, continuous verification, and multi-factor methods that dynamically adjust based on behavioral or contextual risk signals. By eliminating reliance on static credentials, vendors are helping financial institutions and digital platforms preserve seamless user experiences while reducing credential-based fraud.

Behavioral and Device Intelligence

Top vendors are expanding detection capabilities through behavioral biometrics, device fingerprinting, and session analytics. These tools monitor how users type, move, and interact, identifying subtle deviations that may indicate account compromise. When combined with device and network intelligence, they enable proactive identification of unauthorized access attempts before funds or data are exposed. This layered intelligence approach strengthens ongoing session security across digital banking, eCommerce, and payment ecosystems.

AI-Driven Threat Detection and Response

Next-generation ATO solutions leverage artificial intelligence and machine learning to recognize complex and evolving attack vectors such as deepfakes, credential stuffing, and synthetic identities. These systems continuously tune detection models to adapt to new threats, providing early warning and automated incident response. By integrating AI-driven defense across authentication and fraud workflows, leading vendors are transforming reactive account protection into real-time, predictive security.



04

Vendor Overview

Entersekt

About Entersekt

Founded in 2008, Entersekt specializes in digital banking security, strong authentication, and 3DS Authentication. The company's mission is to eliminate the friction between secure authentication and seamless digital experiences for financial institutions and merchants. Entersekt's platform delivers passwordless and silent options, phishing-resistant authentication across mobile, web, and call center channels, supporting compliance with PSD2 and FIDO standards. Trusted by major banks and card issuers, Entersekt enables risk-based, context-aware authentication, empowering clients to prevent account takeover and identity fraud while maintaining user convenience.

Company Information (as of November 2025)

Headquarters	Atlanta, Georgia
No. of Employees	257
Last Raised	Private Equity Funding in January 2023
Market Cap	–
Industry Focus	Financial Services
Geographic Focus	North America, Europe
Notable Customers	Investec, Cash App, CAPITEC

■ Exceptional ▣ Excellent □ Strong

1 The Exceptional, Excellent, and Strong scoring buckets are relative to the performance of only the leading vendor for Account Takeover Prevention in Banking. Vendors outside the scoring buckets are not considered leading vendors for Account Takeover Prevention in Banking.

Liminal

Performance on Account Takeover Link Index Benchmarking Criteria

Avg.	Criteria		Performance[1]
□ Strategy	**Ease of Implementation**	The effort required to deploy the solution across systems. Prebuilt integrations reduce setup time and complexity.	□
	End-Customer Experience	The solution's ability to secure users while keeping friction low, supporting trust, and reducing abandonment.	▣
	Scalability	The solution's capacity to handle rising transaction volumes and fraud complexity while maintaining accuracy and reliability.	□
	Orchestration and Platform Approach	The solution's ability to unify tools and data for coordinated, flexible fraud and identity management.	■
■ Product	**ATO Capability Coverage**	The range of features supporting ATO prevention, detection, and recovery across user accounts and transactions.	■
	Buyer Satisfaction	The satisfaction level among users, reflecting solution performance, reliability, and alignment with buyer needs.	■
	Generative AI Guardrails	The defenses protecting against AI-driven ATO threats such as synthetic identities and manipulated content.	▣
	Data Quality and Integrity	The completeness, accuracy, and timeliness of account and identity data used for ATO detection and response.	▣
	Post-ATO Recovery Process	The tools supporting secure user re-entry, remediation, and restoration after a confirmed ATO incident.	▣
	Authentication Flow Adaptability	The flexibility to adjust authentication dynamically using contextual and risk-based indicators.	▣
□ Market Presence	**Company Size**	The total number of employees within the organization, indicating overall operational scale and service capacity.	□
	Employee Growth	The year-over-year rate of change in employee count, showing organizational growth and scalability potential.	□
	Market Leadership Perception	The percentage of buyers identifying the vendor as a leader, showing market strength and reputation.	▣
	Funding History	The total capital raised reflects financial stability, investor backing, and the market's growth potential.	▣
	Digital Footprint	The company's visibility and engagement across online platforms, indicating reach and digital market influence.	□
	Media Coverage	The frequency and credibility of media mentions, reflecting visibility, recognition, and perceived market influence.	□

Entersekt

Analyst Notes

The Entersekt Secure Platform provides a comprehensive, multi-layered framework for ATO prevention, combining device intelligence, push-based authentication, and cryptographic identity binding. By replacing legacy one-time passwords (OTPs) with passwordless authentication and biometric verification, the solution strengthens defense against phishing and SIM-swap attacks.[2] Its contextual risk engine continuously evaluates behavioral and device signals to detect anomalies in real time, delivering protection without compromising user experience. Entersekt's API-based architecture enables scalable integration with digital banking ecosystems, allowing banks to unify authentication across all channels.[2] The platform's adaptive authentication dynamically adjusts challenge levels based on assessed risk, minimizing friction while ensuring secure account access. These capabilities align with an industry-wide recognition that authentication remains the most effective control for reducing ATO risk, with 97% of practitioners confirming its ability to lower exposure.[1]

Entersekt's go-to-market strategy centers on helping FIs modernize authentication infrastructures and replace high-friction methods with seamless, customer-first security experiences. The company emphasizes migration from SMS OTPs to cryptographically protected push notifications and passkeys, meeting both customer expectations and regulatory mandates. Pricing is structured around a modular SaaS model, allowing clients to activate components such as risk-based authentication or transaction signing as their business needs evolve. The platform supports integration through SDKs and APIs for mobile and digital channels, promoting rapid deployment and extensibility.[2] Entersekt's strategic alliances, such as its collaboration with Mastercard on the Scam Protect initiative, position it as a trusted partner for banks prioritizing fraud resilience.[2] Its roadmap aligns with market trends, emphasizing automation, scalable recovery, and orchestration—areas where 81% of practitioners now favor automated re-verification workflows over manual reviews.[1]

Entersekt maintains a strong footprint across Europe, the Middle East, Africa (EMEA), and North America, with expanding engagements in APAC through partnerships with global payment networks and regional banks. Its authentication technology underpins large-scale implementations for banks with customer bases exceeding eight million users, illustrating its scalability.[2] The broader ATO market context supports this growth trajectory, as 88% of buyers now prefer unified authentication and orchestration platforms to consolidate threat mitigation.[1] The firm's global partnerships and ecosystem integrations—particularly through FIDO, Mastercard, and major core banking vendors—continue to strengthen its positioning as a leading provider of modern, passwordless authentication solutions for the prevention of account takeover fraud.[2]

● High ◉ Medium ○ Low

1 Third Party Fraud Buyer Demand Survey, August 2025 (N=73)
2 Entersekt, "Safeguard your FI against the reputational and financial losses of account takeover fraud."
3 Greyed out capabilities are not offered with the vendor solution.

Account Takeover Capabilities[3]

Requirements to Satisfy the Use Case		Buyer Demand for Product Capability[1]
Authenticate Customer Accounts	Verifies that a user accessing a system is the legitimate owner of the account. This typically involves validating identity credentials, such as passwords, multi-factor authentication (MFA), biometric data, or one-time passcodes, at the time of login or during sensitive transactions. The goal is to ensure only authorized users can access or modify account information, protecting against unauthorized access, fraud, and identity theft.	App-Based Authentication ● Multi-Factor Authentication (MFA) ● Biometric Authentication ◉ Continuous Authentication ◉ Adaptive Authentication ○ Passwordless Authentication ○
Detect Anomalous Behavioral Activity for Fraud Threats	Analyzes user behavior to identify actions that deviate from typical patterns and may indicate fraudulent intent. By detecting these anomalies in real time, organizations can flag potential first-party, third-party, or synthetic identity fraud before it results in financial loss.	Data Breach Monitoring Location Intelligence ● Behavioral Biometrics ◉ Device Health Status Detection SIM Swap Detection ◉ Social Engineering and Scam Detection ◉ Behavioral Analytics ○ Bot Detection ○
Detect Suspicious Transactions for Fraud	Analyzes transaction data for anomalies, patterns, and behaviors indicative of fraud. This capability involves monitoring transactions in real-time or near real-time using rule-based engines, machine learning models, or behavioral analytics to flag unusual activity, such as sudden changes in spending, high-risk geographies, or rapid movement of funds.	Behavioral Biometrics ◉ Fraud Monitoring ◉ Location Intelligence ◉ Behavioral Analytics ○
Enable Identity Self-Service Capabilities	Provides users with the tools to manage their own identity-related tasks, such as resetting passwords, updating personal information, or managing access permissions. This requirement enhances user experience by offering convenience and reducing the burden on IT support, while still maintaining security and compliance standards.	Customer Identity Self-Service capabilities ◉
Trigger Dynamic Authentication Based on User Risk	Adjusts the level of authentication required based on the perceived risk associated with a user's actions. This requirement enhances security by requiring additional verification steps, such as multi-factor authentication, when unusual or high-risk activities are detected.	Endpoint and Device Behavioral Analytics ● App-Based Authentication ◉ Behavioral Analytics ◉ Behavioral Biometrics ◉ Continuous Authentication ◉ Location Intelligence ◉ Multi-Factor Authentication (MFA) ◉ Adaptive Authentication ○ Passwordless Authentication ○



05

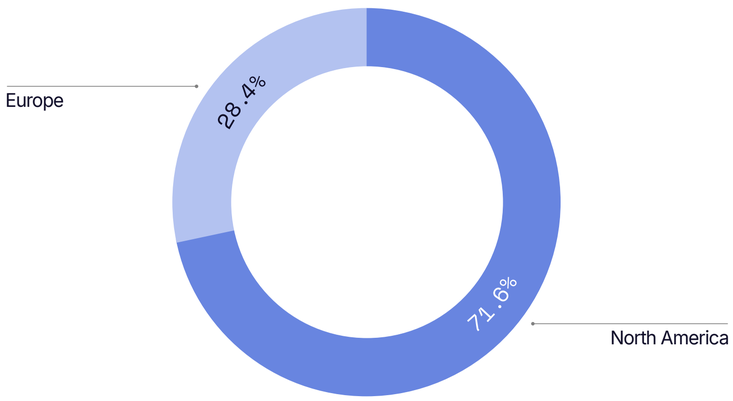
Appendix

Market Presence Survey Demographics

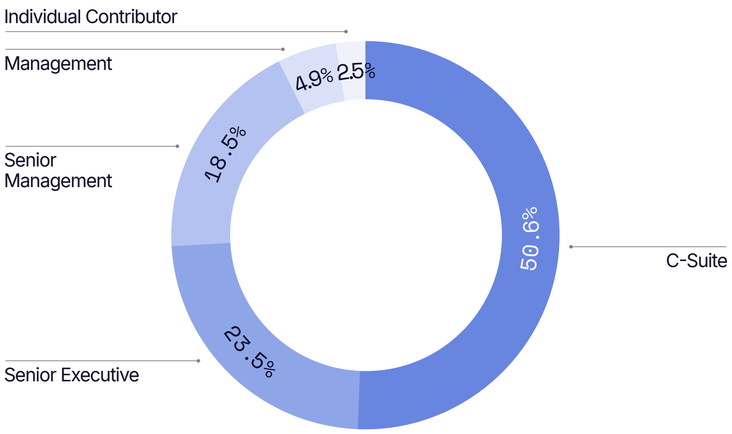
Survey Respondent Demongraphics (N=81)[1]

Geography

By Region, highest priority based on revenue

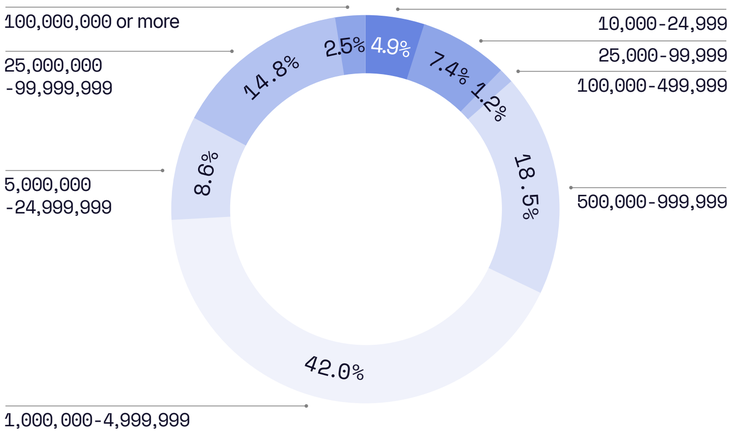


Job Level



Company Size

By Customers



1 Third Party Fraud Buyer Demand Survey, August 2025 (N=81)

Link Index Methodology

Exceptional, Excellent, Strong Scoring Buckets Definitions

Scoring Buckets	Definition
Exceptional	Vendors in this category demonstrate the highest level of performance in the ATO prevention market, ranking above the third quartile among leading providers. These vendors exceed regulatory and industry expectations by delivering advanced fraud orchestration, adaptive authentication, policy enforcement, and scalable incident response capabilities. Their platforms support seamless integration across customer-facing channels, facilitate compliance with regulations such as GDPR and CCPA, and improve customer trust by detecting threats early and securing accounts against compromise.
Excellent	Vendors in this tier offer highly capable ATO prevention solutions, ranking between the first and third quartile among top providers. They provide strong account monitoring, threat detection, and fraud response features, with support for configurable policies and integration with security operations. While they may not offer the same breadth of advanced analytics or orchestration tools as Exceptional vendors, these solutions improve detection accuracy, strengthen operational capability, and support regulatory compliance, making them suitable for organizations seeking reliable and adaptable fraud prevention.
Strong	Vendors in this category meet core ATO prevention requirements, ranking below the first quartile among leading providers while surpassing baseline offerings. Their platforms include essential capabilities such as suspicious login detection, basic multi-factor authentication, and account activity monitoring. Although they may lack extensive integration support, advanced analytics, or adaptive policy management, their solutions remain appropriate for institutions prioritizing foundational fraud detection and prevention aligned with basic regulatory and security standards.

Product Capability Definitions

Capability	Definition
Adaptive Authentication	Adaptive authentication (also known as risk-based authentication or context-based authentication) is the process of authenticating a user based on the risk level presented by a login attempt.
App-Based Authentication	App-based authentication, such as the use of an authenticator app, is a method that provides an additional layer of security for online accounts through multi-factor authentication (MFA). These apps generate time-based, one-time passcodes (TOTP or OTP) on a user's smartphone, which must be entered in addition to the usual login credentials (like a password) to gain access to an account.
Behavioral Analytics	Behavioral analytics is a data analysis process that focuses on understanding how users interact with systems and applications to detect unusual behaviors that may indicate security threats or unauthorized activities. It tracks and analyzes a wide range of user activities - from account creation and form submissions to purchasing behavior - to glean insights into user preferences, habits, and intentions.
Behavioral Biometrics	Behavioral biometrics identifies individuals based on their unique patterns of behavior, particularly in the context of human-computer interaction. Unlike physical biometrics, which rely on innate physical characteristics like fingerprints or iris patterns, behavioral biometrics focuses on patterns that emerge from a person's natural interactions and activities, such as typing rhythm, mouse movements, gait, and voice dynamics.
Biometric Authentication	Biometric authentication refers to a process that verifies a user’s identity using their unique biological traits such as fingerprints, voices, retinas, and facial features. Biometric authentication can use both physical biometrics (based on physiological features) and behavioral biometrics (based on how people behave).
Bot Detection	Bot detection involves identifying entities or individuals that mimic user behavior, such as bots, malware, or rogue applications, which may attempt to evade traditional security tools by blending in with normal user activities like browsing the web or sending emails. It also refers to a process of analyzing traffic to a website, mobile application, or API to detect and block malicious bots.

Product Capability Definitions

Capability	Definition
Continuous Authentication	Continuous authentication is a security approach that verifies a user's identity continuously throughout a session, rather than just at the point of login.
Customer Identity Self-Service capabilities	Customer Identity Self-Service capabilities refer to the features and functionalities that enable customers to manage their own identity information and account settings without the need for direct assistance from customer support or administrators.
Data Breach Monitoring	Data breach monitoring is a threat detection service that alerts users when one of their accounts and associated data has been leaked in a data breach. It involves tracking compromised personal information on the dark web and other illicit platforms to prevent identity theft.
Device Health Status Detection	Device health status detection includes monitoring devices' health and security status to ensure they are protected against threats. It involves the analysis of a device to assess its security hygiene by identifying jailbroken devices, hardware modifications, and/or malicious code.
Endpoint & Device Behavior Analytics	Device behavior intelligence involves analyzing the activities and behaviors of devices to detect anomalies and potential security threats. It helps identify suspicious behavior patterns that may indicate compromised devices or malicious activities.
Fraud Monitoring	Fraud monitoring is the surveillance and analysis of networks, accounts, and transactions to identify potentially fraudulent activity for automated fraud decisioning.

Product Capability Definitions

Capability	Definition
Location Intelligence	Location intelligence leverages geolocation data to understand user behavior, deliver personalized services, and enhance marketing strategies based on real-time location information.
Multi-factor Authentication	Multi-factor Authentication (MFA) is a security process that requires users to provide two or more verification factors to gain access to a resource such as an application, online account, or VPN. It enhances security by combining multiple methods of authentication, reducing the risk of unauthorized access.
Passwordless Authentication	Passwordless authentication is a security process that allows users to access their accounts without the need for a traditional password. Instead, it uses alternative methods such as biometrics, email or SMS codes, or hardware tokens to verify the user’s identity.
SIM Swap Detection	SIM Swap Detection is a security process used to identify and prevent SIM swap fraud, a type of identity theft where a fraudster manages to transfer a victim's phone number to a new SIM card they control.
Social Engineering and Scam Detection	Social engineering and scam detection involves rules-based or machine-learning models configured to identify customer behavior indicative of social engineering. Social engineering involves manipulating individuals to divulge sensitive information or perform actions that aid fraudsters in gaining unauthorized access to data or systems. Scam detection refers to identifying and preventing fraudulent schemes designed to deceive individuals into providing personal information or financial assets.

Link Index Methodology

Product

Product Criteria	Weighting	Definition	Why It Matters
ATO Capabilities	60.00%	The breadth of capabilities a vendor offers to address the requirements of this use case.	The range of capabilities determines how effectively a vendor can detect, prevent, and respond to different ATO attack vectors across user accounts and digital channels.
Buyer Satisfaction	15.00%	The extent of buyer satisfaction with a vendor's solution.	High satisfaction reflects the reliability and perceived value of the solution in real-world ATO prevention scenarios, indicating strong performance and usability.
Generative AI Guardrails	5.00%	Evaluates defenses against AI-driven ATO threats, including manipulated content and synthetic identities.	Defenses against AI-generated threats are essential as attackers increasingly use synthetic content and deepfakes to bypass identity and access controls.
Data Quality & Integrity	5.00%	Reviews the accuracy, completeness, and timeliness of account, transaction, and identity data used for ATO detection and response.	Accurate and timely data supports reliable ATO detection, ensuring that alerts and decisions are based on trustworthy signals rather than false positives or incomplete records.
Post-ATO Recovery Process	5.00%	Examines mechanisms for user re-entry and remediation following a confirmed ATO incident.	Effective recovery processes restore legitimate user access while minimizing downtime and reputational harm after an account has been compromised.
Authentication Flow Adaptability	10.00%	Assesses how dynamic and context-aware authentication methods are in mitigating ATO risk. Goes beyond basic MFA to adaptive, risk-based flows.	Dynamic, context-aware authentication strengthens ATO prevention by adjusting verification measures in real time based on user behavior and risk signals.

Link Index Methodology

Strategy

Strategy Criteria	Weighting	Definition	Why It Matters
Ease of Implementation	25.00%	Assesses the level of effort required to deploy the solution across key systems such as payment gateways, CRMs, and fraud platforms. Prebuilt integrations and streamlined onboarding reduce deployment complexity and shorten time to value.	Low implementation complexity enables faster deployment across existing systems, allowing organizations to protect accounts against takeover threats without disrupting critical operations.
End-Customer Experience	25.00%	Measures the solution's ability to protect accounts without creating friction for legitimate users. A consistent and fair experience strengthens customer trust and reduces abandonment.	Maintaining low friction for legitimate users reduces login frustration and account lockouts, preserving trust while still defending against malicious access attempts.
Scalability	25.00%	Evaluates the solution's capacity to support increasing transaction volumes and adapt to evolving fraud tactics. Scalable solutions maintain performance and accuracy as customer bases and attack surfaces expand.	A scalable solution ensures consistent detection and prevention of ATO attacks as transaction volumes, user activity, and threat sophistication increase.
Orchestration / Platform Approach	25.00%	Reviews whether the solution functions as a broader platform versus a single-point tool. Platforms provide unified coverage across multiple fraud and identity use cases, while orchestration allows integration with third-party vendors.	A platform-based or orchestrated solution enables unified fraud prevention by integrating ATO defenses with other identity and risk tools, improving visibility and response coordination.

Link Index Methodology

Market Presence

Market Criteria	Weighting	Definition	Why It Matters
Company Size	20.00%	The total employee headcount of a company.	A larger workforce often indicates greater operational capacity, enabling sustained product development and customer support.
Employee Growth (YoY)	20.00%	How fast a company's employee count is growing.	Rapid employee growth signals business expansion and investment in capability building, reflecting overall organizational momentum.
Market Leadership Perception	20.00%	The number of buyers who believe this vendor is a market leader.	Strong market perception enhances credibility and buyer confidence, influencing vendor selection and partnership opportunities.
Funding History	30.00%	Total funding a company has incurred.	Adequate funding supports long-term stability, innovation, and scalability, ensuring the vendor can sustain product improvement and client needs.
Digital Footprint	5.00%	The company’s total social media footprint.	A strong online presence increases visibility, engagement, and perceived relevance in the chargeback prevention market.
Media Coverage	5.00%	Vendor mentions/quotes in authoritative outlets reflect market presence.	Frequent and credible media mentions demonstrate thought leadership, validate market influence, and reinforce trust among prospective buyers.

Liminal™

From Research to Revenue - The Actionable Intelligence Platform



The same depth and rigor you've just read, now powering your real-time link between strategy and execution

Unify market, competitor, and buyer intelligence to power every motion - from sales execution to product strategy. With Liminal, your GTM team will always know where to play and how to win.

Discover

map vendors, products, and use-cases to reveal actionable whitespace, monitor in real-time

Position

target with precision: 35k+ personas continuously refreshed with in-market buyer intelligence

Mobilize

connect deeply, quickly, and at scale with dynamic battlecards and personalized prospect outreach

Execute

close faster and win more with deal-level insights embedded across your workflow





GTM teams using Liminal **close more deals**

Proven across our portfolio

30%

higher win rates

See how Liminal elevates research into results - actionable intelligence from discovery to close.

Book a Demo

Liminal™

link Index™ Report

Liminal Strategy, Inc.
825 Third Avenue, Suite 1700, New York, NY 10022

www.liminal.co | info@liminal.co

Copyright © 2026 Liminal Strategy, Inc. | www.liminal.co
This report may not be reproduced without permission from Liminal | Citation Policy